

Unifying notions of generalized weights for universal security on wire-tap networks

Umberto Martínez-Peñas

Department of Mathematical Sciences, Aalborg University, Denmark

Email: umberto@math.aau.dk

and

Ryutaroh Matsumoto

Department of Information and Communications Engineering, Tokyo Institute of Technology, Japan.

Abstract—Universal security over a network with linear network coding has been intensively studied. However, previous linear codes used for this purpose were linear over a larger field than that used on the network. In this work, we introduce new parameters (relative dimension/rank support profile and relative generalized matrix weights) for linear codes that are linear over the field used in the network, measuring the universal security performance of these codes. The proposed new parameters enable us to use optimally universal secure linear codes on noiseless networks for all possible parameters, as opposed to previous works, and also enable us to add universal security to the recently proposed list-decodable rank-metric codes by Guruswami et al. We give several properties of the new parameters: monotonicity, Singleton-type lower and upper bounds, a duality theorem, and definitions and characterizations of equivalences of linear codes. Finally, we show that our parameters strictly extend relative dimension/length profile and relative generalized Hamming weights, respectively, and relative dimension/intersection profile and relative generalized rank weights, respectively. Moreover, we show that generalized matrix weights are larger than Delsarte generalized weights.

I. INTRODUCTION

Linear network coding was first studied in [1], [2] and [16], and allows to realize higher throughput than the conventional storing and forwarding. In this context, security over the network, meaning information leakage to a wire-tapping adversary, was first considered in [3] and later in [6]. However, both approaches require knowing and/or modifying the underlying linear network code, which does not allow to perform, for instance, random linear network coding [12].

The use of outer coding on the source node was proposed in [7] to protect messages from information leakage knowing but without modifying the underlying linear network code. Later, the use of linear (block) codes as outer codes was proposed in [25] to protect messages from errors together with information leakage to a wire-tapping adversary, depending only on the number of errors and wire-tapped links, and not depending on the underlying linear network code, which was there referred to as “universal security”. In particular, optimal parameters are obtained in [25] for universal security over noiseless networks for some restricted packet lengths.

This approach was further investigated in [15], where relative generalized rank weights (RGRWs) and relative

dimension/intersection profiles (RDIPs) were introduced to measure simultaneously the universal security performance and correction capability of pairs of linear codes, which are used for coset coding as in [28].

Unfortunately, the codes proposed in [25] and [15] are linear over the finite field \mathbb{F}_{q^m} , where m is the packet length, if the linear network coding is performed over the finite field \mathbb{F}_q . This restricts the achievable parameters, requires performing computations over the larger field \mathbb{F}_{q^m} and leaves out important codes, such as the codes obtained in [11], which are the first list-decodable rank-metric codes whose list sizes are polynomial in the code length. Moreover, even though there exist maximum rank distance codes (see [5]), and hence optimally universal secure codes for noiseless networks, that can be applied for all number of outgoing links from the source, all packet lengths and all dimensions over \mathbb{F}_q , the maximum rank distance codes considered in [25] and [15] only include Gabidulin codes [9] and some reducible codes [10], for which the previous parameters are restricted.

In this work, we study the universal security performance of codes and coset coding schemes that are linear over the smaller field \mathbb{F}_q . After some preliminaries in Section II, the new contributions of this paper are organized as follows:

In Section III, we introduce relative dimension/rank support profiles (RDRPs) and relative generalized matrix weights (RGMWs) and give their monotonicity properties. In Section IV, we prove that RDRPs and RGMWs exactly measure the worst case information leakage on networks, and then we give optimal linear coset coding schemes for noiseless networks for all possible parameters, in contrast to previous works. In Section V, we show how to add universal security to the list-decodable codes in [11] using linear coset coding schemes and the study in the previous sections. In Section VI, we study basic properties of RDRPs and RGMWs: Upper and lower Singleton-type bounds and the duality theorem for GMWs. In Section VII, we define and study security equivalences of linear codes, and then obtain ranges of possible parameters and minimum parameters of linear codes up to these equivalences. Finally, in Section VIII, we prove that RDRPs strictly extend RDLs [8], [17] and RDIPs [15],

and we prove that RGMWs strictly extend RGHws [17], [27] and RGRWs [15]. We conclude by showing that GMWs are larger (strictly in some cases) than Delsarte generalized weights [23].

Due to space limitations, some proofs are omitted. They can be found in the extended version [19].

II. COSET CODING SCHEMES FOR UNIVERSAL SECURITY IN LINEAR NETWORK CODING

A. Notation

Let q be a prime power and m and n , two positive integers. We denote by \mathbb{F} an arbitrary field and by \mathbb{F}_q the finite field with q elements. \mathbb{F}^n denotes the vector space of row vectors of length n with components in \mathbb{F} , and $\mathbb{F}^{m \times n}$ denotes the vector space of $m \times n$ matrices with components in \mathbb{F} . For a vector space \mathcal{V} over \mathbb{F} and a subset $\mathcal{A} \subseteq \mathcal{V}$, we denote by $\langle \mathcal{A} \rangle$ the vector space generated by \mathcal{A} over \mathbb{F} , and we denote by $\dim(\mathcal{V})$ the dimension of \mathcal{V} over \mathbb{F} . Finally, $A^T \in \mathbb{F}^{n \times m}$ denotes the transposed of a matrix $A \in \mathbb{F}^{m \times n}$, $\text{Rk}(A)$ denotes its rank, and the symbols $+$ and \oplus denote the sum and direct sum of vector spaces, respectively.

Throughout the paper, a (block) code in $\mathbb{F}^{m \times n}$ (respectively, in \mathbb{F}^n) is a subset of $\mathbb{F}^{m \times n}$ (respectively, of \mathbb{F}^n), and it is called linear if it is a vector space.

B. Linear network coding model

Consider a network with several sources and several sinks. A given source transmits a message $\mathbf{x} \in \mathbb{F}_q^\ell$ through the network to multiple sinks. To that end, that source encodes the message as a collection of n packets of length m , seen as a matrix $C \in \mathbb{F}_q^{m \times n}$, where n is the number of outgoing links from this source. We consider linear network coding on the network, first considered in [1], [16] and formally defined in [14, Definition 1], which allows to reach higher throughput than just storing and forwarding on the network. This means that a given sink receives a matrix of the form

$$Y = CA^T \in \mathbb{F}_q^{m \times N},$$

where $A \in \mathbb{F}_q^{N \times n}$ is called the transfer matrix corresponding to the considered source and sink. This matrix may be randomly chosen if random linear network coding is applied [12].

C. Universal secure communication over networks

In secure or reliable network coding, two of the main problems addressed in the literature are the following:

- 1) Error and erasure correction [15], [24], [25]: An adversary and/or a noisy channel may introduce errors on some links of the network and/or modify the transfer matrix, hence the sink receives the matrix

$$Y = CA'^T + E \in \mathbb{F}_q^{m \times N},$$

where $A' \in \mathbb{F}_q^{N \times n}$ is the modified transfer matrix, and $E \in \mathbb{F}_q^{m \times N}$ is the final error matrix. We say that $t = \text{Rk}(E)$ errors and $\rho = n - \text{Rk}(A')$ erasures occurred.

- 2) Information leakage [3], [6], [7], [15], [25]: A wire-tapping adversary listens to $\mu > 0$ links of the network,

obtaining a matrix of the form $CB^T \in \mathbb{F}_q^{m \times \mu}$, for some matrix $B \in \mathbb{F}_q^{\mu \times n}$.

Outer coding in the source node is usually applied to tackle the previous problems, and it is called “universal secure” [25] if it provides security as in the previous items for fixed numbers of wire-tapped links μ , errors t and erasures ρ , independently of the transfer matrix A used. This implies that no previous knowledge or modification of the transfer matrix is required and random linear network coding [12] may be applied.

D. Coset coding schemes for outer codes

The concept of coset coding scheme was introduced in [28] to protect messages simultaneously from errors and information leakage. We use the formal definition [15, Definition 7]:

Definition 1 (Coset coding schemes [15], [28]). A coset coding scheme over the field \mathbb{F} with message set \mathcal{S} is a family of disjoint nonempty subsets of $\mathbb{F}^{m \times n}$, $\mathcal{P}_{\mathcal{S}} = \{\mathcal{C}_{\mathbf{x}}\}_{\mathbf{x} \in \mathcal{S}}$.

Each $\mathbf{x} \in \mathcal{S}$ is encoded by the source by choosing uniformly at random an element $C \in \mathcal{C}_{\mathbf{x}}$.

In this paper, we will consider the particular case obtained by using nested linear code pairs, introduced in [29, Section III.A]:

Definition 2 (Nested linear code pairs [29]). A nested linear code pair is a pair of linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$. Choose a vector space \mathcal{W} such that $\mathcal{C}_1 = \mathcal{C}_2 \oplus \mathcal{W}$ and a vector space isomorphism $\psi : \mathbb{F}^\ell \rightarrow \mathcal{W}$, where $\ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$. Then we define the sets $\mathcal{C}_{\mathbf{x}} = \psi(\mathbf{x}) + \mathcal{C}_2$, for $\mathbf{x} \in \mathbb{F}^\ell$.

These coset coding schemes are linear in the following sense:

$$a\mathcal{C}_{\mathbf{x}} + b\mathcal{C}_{\mathbf{y}} \subseteq \mathcal{C}_{a\mathbf{x}+b\mathbf{y}},$$

for all $a, b \in \mathbb{F}$ and all $\mathbf{x}, \mathbf{y} \in \mathbb{F}^\ell$. Moreover, they are the only coset coding schemes with this linearity property (see [18, Proposition 1]).

III. NEW PARAMETERS OF LINEAR COSET CODING SCHEMES FOR UNIVERSAL SECURITY ON NETWORKS

Inspired by [13], [15], [18], we define rank supports and rank support spaces as follows:

Definition 3 (Row space and rank). For a matrix $C \in \mathbb{F}^{m \times n}$, we define its row space $\text{Row}(C)$ as the vector space in \mathbb{F}^n generated by its rows, and its rank as $\text{Rk}(C) = \dim(\text{Row}(C))$.

Definition 4 (Rank support and rank weight [13, Definition 1]). Given a vector space $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$, we define its rank support as

$$\text{RSupp}(\mathcal{C}) = \sum_{C \in \mathcal{C}} \text{Row}(C) \subseteq \mathbb{F}^n.$$

We also define the rank weight of the space \mathcal{C} as

$$\text{wt}_{\text{R}}(\mathcal{C}) = \dim(\text{RSupp}(\mathcal{C})).$$

Obviously, $\text{RSupp}(\langle \{C\} \rangle) = \text{Row}(C)$ and $\text{wt}_{\text{R}}(\langle \{C\} \rangle) = \text{Rk}(C)$, for every matrix $C \in \mathbb{F}^{m \times n}$.

Definition 5 (Rank support spaces). Given a vector space $\mathcal{L} \subseteq \mathbb{F}^n$, we define its rank support space $\mathcal{V}_{\mathcal{L}} \subseteq \mathbb{F}^{m \times n}$ as

$$\mathcal{V}_{\mathcal{L}} = \{V \in \mathbb{F}^{m \times n} \mid \text{Row}(V) \subseteq \mathcal{L}\}.$$

We denote by $RS(\mathbb{F}^{m \times n})$ the family of rank support spaces in $\mathbb{F}^{m \times n}$.

A proof of the following result can be found in [19]:

Theorem 1. Fix a set $\mathcal{V} \subseteq \mathbb{F}^{m \times n}$. The following are equivalent:

- 1) \mathcal{V} is a rank support space. That is, there exists a subspace $\mathcal{L} \subseteq \mathbb{F}^n$ such that $\mathcal{V} = \mathcal{V}_{\mathcal{L}}$.
- 2) \mathcal{V} is linear and has a basis of the form $B_{i,j}$, for $i = 1, 2, \dots, m$ and $j = 1, 2, \dots, k$, where there are vectors $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_k \in \mathbb{F}^n$ such that $B_{i,j}$ has the vector \mathbf{b}_j in the i -th row and the rest of its rows are zero vectors.
- 3) There exists a matrix $B \in \mathbb{F}^{\mu \times n}$, for some positive integer μ , such that

$$\mathcal{V} = \{V \in \mathbb{F}^{m \times n} \mid VB^T = 0\}.$$

In addition, the relation between items 1, 2 and 3 is that $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_k$ are a basis of \mathcal{L} , B is a (possibly not full-rank) parity check matrix of \mathcal{L} and $\dim(\mathcal{L}) = n - \text{Rk}(B)$. In particular,

$$\dim(\mathcal{V}_{\mathcal{L}}) = m \dim(\mathcal{L}). \quad (1)$$

We conclude by studying the duality of rank support spaces. We consider the following inner product in $\mathbb{F}^{m \times n}$:

Definition 6 (Hilbert-Schmidt or trace product). Given matrices $C, D \in \mathbb{F}^{m \times n}$, we define its Hilbert-Schmidt product, or trace product, as

$$\begin{aligned} \langle C, D \rangle &= \text{Trace}(CD^T) \\ &= \sum_{i=1}^m \mathbf{c}_i \cdot \mathbf{d}_i = \sum_{i=1}^m \sum_{j=1}^n c_{i,j} d_{i,j} \in \mathbb{F}, \end{aligned}$$

where \mathbf{c}_i and \mathbf{d}_i are the rows of C and D , respectively, and where $c_{i,j}$ and $d_{i,j}$ are their components, respectively.

Given a vector space $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$, we denote by \mathcal{C}^\perp its dual:

$$\mathcal{C}^\perp = \{D \in \mathbb{F}^{m \times n} \mid \langle C, D \rangle = 0, \forall C \in \mathcal{C}\}.$$

Since the trace product in $\mathbb{F}^{m \times n}$ coincides with the usual inner product in \mathbb{F}^{mn} , it holds that

$$\begin{aligned} \dim(\mathcal{C}^\perp) &= mn - \dim(\mathcal{C}), \quad \mathcal{C} \subseteq \mathcal{D} \iff \mathcal{D}^\perp \subseteq \mathcal{C}^\perp, \\ \mathcal{C}^{\perp\perp} &= \mathcal{C}, \quad (\mathcal{C} + \mathcal{D})^\perp = \mathcal{C}^\perp \cap \mathcal{D}^\perp, \quad (\mathcal{C} \cap \mathcal{D})^\perp = \mathcal{C}^\perp + \mathcal{D}^\perp, \end{aligned}$$

for linear codes $\mathcal{C}, \mathcal{D} \subseteq \mathbb{F}^{m \times n}$. We also have the following:

Proposition 1. If $\mathcal{V} \in RS(\mathbb{F}^{m \times n})$, then $\mathcal{V}^\perp \in RS(\mathbb{F}^{m \times n})$. More concretely, for any subspace $\mathcal{L} \subseteq \mathbb{F}^n$, it holds that

$$(\mathcal{V}_{\mathcal{L}})^\perp = \mathcal{V}_{(\mathcal{L}^\perp)}.$$

With these tools, we may now define the new parameters:

Definition 7 (Relative Dimension/Rank support Profile). Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$, and $0 \leq \mu \leq n$, we define their μ -th relative dimension/rank support profile

(RDRP) as

$$K_{M,\mu}(\mathcal{C}_1, \mathcal{C}_2) = \max\{\dim(\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}}) - \dim(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}}) \mid \mathcal{L} \subseteq \mathbb{F}^n, \dim(\mathcal{L}) \leq \mu\}.$$

Definition 8 (Relative Generalized Matrix Weight). Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$, and $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$, we define their r -th relative generalized matrix weight (RGMW) as

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{\dim(\mathcal{L}) \mid \mathcal{L} \subseteq \mathbb{F}^n, \dim(\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}}) - \dim(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}}) \geq r\}.$$

For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$, and $1 \leq r \leq \dim(\mathcal{C})$, we define its r -th generalized matrix weight (GMW) as

$$d_{M,r}(\mathcal{C}) = d_{M,r}(\mathcal{C}, \{0\}). \quad (2)$$

We next obtain the following characterization of RGMWs that gives an analogous description to the original definition of generalized Hamming weights by Wei [27]:

Theorem 2. Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$, and an integer $1 \leq r \leq \dim(\mathcal{C}_1/\mathcal{C}_2)$, it holds that

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{\text{wt}_R(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C}_1, \mathcal{D} \cap \mathcal{C}_2 = \{0\}, \dim(\mathcal{D}) = r\}.$$

In particular, it holds that

$$d_{M,1}(\mathcal{C}_1, \mathcal{C}_2) = d_R(\mathcal{C}_1, \mathcal{C}_2) = \min\{\text{Rk}(C) \mid C \in \mathcal{C}_1, C \notin \mathcal{C}_2\}.$$

Proof: Denote by d_r and d'_r the left-hand and right-hand sides of the first equality, respectively.

First, take a vector space $\mathcal{D} \subseteq \mathcal{C}_1$ such that $\mathcal{D} \cap \mathcal{C}_2 = \{0\}$, $\dim(\mathcal{D}) = r$ and $\text{wt}_R(\mathcal{D}) = d'_r$. Define $\mathcal{L} = \text{RSupp}(\mathcal{D})$.

Since $\mathcal{D} \subseteq \mathcal{V}_{\mathcal{L}}$, we have that $\dim((\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}})/(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}})) \geq \dim((\mathcal{C}_1 \cap \mathcal{D})/(\mathcal{C}_2 \cap \mathcal{D})) = \dim(\mathcal{D}) = r$. Hence

$$d_r \leq \dim(\mathcal{L}) = \text{wt}_R(\mathcal{D}) = d'_r.$$

Conversely, take a vector space $\mathcal{L} \subseteq \mathbb{F}^n$, such that $\dim((\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}})/(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}})) \geq r$ and $\dim(\mathcal{L}) = d_r$.

There exists a vector space $\mathcal{D} \subseteq \mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}}$ with $\mathcal{D} \cap \mathcal{C}_2 = \{0\}$ and $\dim(\mathcal{D}) = r$. We have that $\text{RSupp}(\mathcal{D}) \subseteq \mathcal{L}$, since $\mathcal{D} \subseteq \mathcal{V}_{\mathcal{L}}$, and hence

$$d_r = \dim(\mathcal{L}) \geq \text{wt}_R(\mathcal{D}) \geq d'_r. \quad \blacksquare$$

Finally, we show the monotonicity properties of RDRPs and RGMWs (see [19] for a proof):

Proposition 2 (Monotonicity of RDRPs). Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$, and $0 \leq \mu \leq n - 1$, it holds that $K_{M,0}(\mathcal{C}_1, \mathcal{C}_2) = 0$, $K_{M,n}(\mathcal{C}_1, \mathcal{C}_2) = \dim(\mathcal{C}_1/\mathcal{C}_2)$ and

$$0 \leq K_{M,\mu+1}(\mathcal{C}_1, \mathcal{C}_2) - K_{M,\mu}(\mathcal{C}_1, \mathcal{C}_2) \leq m.$$

Proposition 3 (Monotonicity of RGMWs). Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$ with $\ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$, it holds that

$$0 \leq d_{M,r+1}(\mathcal{C}_1, \mathcal{C}_2) - d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \leq \min\{m, n\},$$

for $1 \leq r \leq \ell - 1$, and

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) + 1 \leq d_{M,r+m}(\mathcal{C}_1, \mathcal{C}_2),$$

for $1 \leq r \leq \ell - m$.

IV. UNIVERSAL SECURITY PERFORMANCE OF LINEAR COSET CODING SCHEMES

A. Measuring information leakage on networks

In this subsection, we consider the problem of information leakage on the network, see Subsection II-C, item 2.

Assume that a given source wants to convey the message $\mathbf{x} \in \mathbb{F}_q^\ell$, which we assume is a random variable with uniform distribution over \mathbb{F}_q^ℓ . Following Subsection II-D, the source encodes \mathbf{x} into a matrix $C \in \mathbb{F}_q^{m \times n}$ using nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$. We also assume that the distributions used in the encoding are all uniform (see Subsection II-D).

According to the information leakage model in Subsection II-C, item 2, a wire-tapping adversary obtains $CB^T \in \mathbb{F}_q^{m \times \mu}$, for some matrix $B \in \mathbb{F}_q^{\mu \times n}$.

In the following proposition, $I(X; Y)$ stands for the mutual information of two random variables X and Y (see [4]).

Proposition 4. *Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$, a matrix $B \in \mathbb{F}_q^{\mu \times n}$, and the uniform random variables \mathbf{x} and CB^T , as in the previous paragraphs, it holds that*

$$I(\mathbf{x}; CB^T) = \dim(\mathcal{C}_2^\perp \cap \mathcal{V}_{\mathcal{L}}) - \dim(\mathcal{C}_1^\perp \cap \mathcal{V}_{\mathcal{L}}), \quad (3)$$

where $\mathcal{L} = \text{Row}(B)$.

Proof: Define the linear map $f : \mathbb{F}_q^{m \times n} \rightarrow \mathbb{F}_q^{m \times \mu}$ by $f(D) = DB^T$, $D \in \mathbb{F}_q^{m \times n}$. It holds that

$$\begin{aligned} H(CB^T) &= H(f(C)) = \log_q(\#f(\mathcal{C}_1)) = \dim(f(\mathcal{C}_1)) \\ &= \dim(\mathcal{C}_1) - \dim(\ker(f) \cap \mathcal{C}_1). \end{aligned}$$

Similarly, for the conditional entropy:

$$H(CB^T | \mathbf{x}) = \dim(\mathcal{C}_2) - \dim(\ker(f) \cap \mathcal{C}_2).$$

It holds that $\ker(f) = \mathcal{V}_{\mathcal{L}^\perp} \subseteq \mathbb{F}_q^{m \times n}$ by Theorem 1. Thus, using $I(\mathbf{x}; CB^T) = H(CB^T) - H(CB^T | \mathbf{x})$, $\ker(f) = \mathcal{V}_{\mathcal{L}^\perp}$ and a dimensions computation, (3) follows. ■

The following theorem follows from the previous proposition, the definitions and Theorem 2:

Theorem 3 (Worst case information leakage). *Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$, and integers $0 \leq \mu \leq n$ and $1 \leq r \leq \dim(\mathcal{C}_1/\mathcal{C}_2)$, it holds that*

- 1) $r = K_{M,\mu}(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp)$ is the maximum information (number of bits multiplied by $\log_2(q)$) about the sent message that can be obtained by wire-tapping at most μ links of the network.
- 2) $\mu = d_{M,r}(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp)$ is the minimum number of links that an adversary needs to wire-tap in order to obtain at least r units of information (number of bits multiplied by $\log_2(q)$) of the sent message.

In particular, $t = d_R(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp) - 1$ is the maximum number of links that an adversary may listen to without obtaining any information about the sent message.

B. Optimal linear coset coding schemes for noiseless networks

In this subsection, we obtain linear coset coding schemes built from nested linear code pairs $\mathcal{C} \subsetneq \mathbb{F}_q^{m \times n}$ with optimal universal security parameters in the case of finite fields $\mathbb{F} = \mathbb{F}_q$. Recall from Subsection II-D that these linear coset coding

schemes are suitable for noiseless networks, as noticed in [21].

Definition 9. For a nested linear code pair of the form $\mathcal{C} \subsetneq \mathbb{F}_q^{m \times n}$, we define its information parameter as $\ell = \dim(\mathbb{F}_q^{m \times n}/\mathcal{C}) = \dim(\mathcal{C}^\perp)$, that is the maximum number of $\log_2(q)$ bits of information that the source can convey, and its security parameter t as the maximum number of links that an adversary may listen to without obtaining any information about the sent message.

We study two problems:

- 1) Find a nested linear code pair $\mathcal{C} \subsetneq \mathbb{F}_q^{m \times n}$ with maximum possible security parameter t when m , n , q and the information parameter ℓ are fixed and given.
- 2) Find a nested linear code pair $\mathcal{C} \subsetneq \mathbb{F}_q^{m \times n}$ with maximum possible information parameter ℓ when m , n , q and the security parameter t are fixed and given.

Thanks to Theorem 3, which implies that $t = d_R(\mathcal{C}^\perp) - 1$, and the Singleton bound on the minimum rank distance [5, Theorem 5.4], we may give upper bounds on the attainable parameters in the previous two problems:

Proposition 5. *Given a nested linear code pair $\mathcal{C} \subsetneq \mathbb{F}_q^{m \times n}$ with information parameter ℓ and security parameter t , it holds that:*

$$\ell \leq \max\{m, n\}(\min\{m, n\} - t), \quad (4)$$

$$t \leq \min\{m, n\} - \left\lceil \frac{\ell}{\max\{m, n\}} \right\rceil. \quad (5)$$

In particular, $\ell \leq mn$ and $t \leq \min\{m, n\}$.

On the other hand, the existence of linear codes in $\mathbb{F}_q^{m \times n}$ attaining the Singleton bound on their dimensions, for all possible choices of m , n and minimum rank distance d_R [5, Theorem 6.3], leads to the following existence result on optimal linear coset coding schemes for noiseless networks.

Theorem 4. *For all choices of positive integers m and n , and all finite fields \mathbb{F}_q , the following hold:*

- 1) For every positive integer $\ell \leq mn$, there exists a nested linear code pair $\mathcal{C} \subsetneq \mathbb{F}_q^{m \times n}$ with information parameter ℓ and security parameter $t = \min\{m, n\} - \lceil (\ell / \max\{m, n\}) \rceil$.
- 2) For every positive integer $t \leq \min\{m, n\}$, there exists a nested linear code pair $\mathcal{C} \subsetneq \mathbb{F}_q^{m \times n}$ with security parameter t and information parameter $\ell = \max\{m, n\}(\min\{m, n\} - t)$.

Remark 1. We remark here that, to the best of our knowledge, only the linear coset coding schemes in item 2 in the previous theorem, for the special case $n \leq m$, have been obtained in the literature. It corresponds to [25, Theorem 7].

Using cartesian products of MRD codes as in [25, Subsection VII-C], linear coset coding schemes as in item 2 in the previous theorem can be obtained when $n > m$, for the restricted parameters $n = lm$ and $\ell = mlk'$, where l and $k' < m$ are positive integers.

Therefore, the previous theorem completes the search for linear coset coding schemes with optimal security parameters

for noiseless networks.

V. UNIVERSAL SECURE LIST-DECODABLE RANK-METRIC LINEAR COSSET CODING SCHEMES

In this section, we will show how to build a nested linear code pair $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$ that can be used to list-decode rank errors, which naturally appear on the network, whose list sizes are polynomial on the code length n , while being universal secure under a given number of wire-tapped links. We will also compare the obtained parameters with those obtained when choosing \mathcal{C}_1 and \mathcal{C}_2 as Gabidulin maximum rank distance (MRD) codes [9].

A. Linear coset coding schemes using Gabidulin MRD codes

Assume that $n \leq m$ and $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$ are MRD linear codes (such as Gabidulin codes [9]) of dimensions $\dim(\mathcal{C}_1) = mk_1$ and $\dim(\mathcal{C}_2) = mk_2$.

The linear coset coding scheme constructed from this nested linear code pair satisfies the following properties:

- 1) The information parameter is $\ell = m(k_1 - k_2)$.
- 2) The security parameter is $t = k_2$.
- 3) If the number of rank errors is $e \leq \lfloor \frac{n-k_1}{2} \rfloor$, then rank error-correction can be performed, giving a unique solution.

B. List-decodable linear coset coding schemes for the rank metric

Assume now that n divides m . For the same positive integers $1 \leq k_2 < k_1 \leq n$ as in the previous subsection, and for fixed $\varepsilon > 0$ and positive integer s , we may construct a linear coset coding scheme from a nested linear code pair $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$, with the following properties:

- 1) The information parameter is $\ell \geq m(k_1 - k_2)(1 - 2\varepsilon)$.
- 2) The security parameter is $t \geq k_2$.
- 3) If the number of rank errors is $e \leq \frac{s}{s+1}(n - k_1)$, then rank-metric list-decoding allows to obtain in polynomial time a list (of uncoded secret messages) of size $q^{O(s^2/\varepsilon^2)}$, which is polynomial in the code length n .

Therefore, we may obtain the same security performance as in the previous subsection, an information parameter that is at least $1 - 2\varepsilon$ times the one in the previous subsection, and can list-decode in polynomial time (with list of polynomial size) roughly $n - k_1$ errors, which is twice as many as in the previous subsection.

Now we show the construction. Fix a basis $\alpha_1, \alpha_2, \dots, \alpha_m$ of \mathbb{F}_q^m as a vector space over \mathbb{F}_q , such that $\alpha_1, \alpha_2, \dots, \alpha_n$ generate \mathbb{F}_q^n . We define the matrix representation map $M_\alpha : \mathbb{F}_q^{m \times n} \rightarrow \mathbb{F}_q^{m \times n}$ associated to the previous basis by

$$M_\alpha(\mathbf{c}) = (c_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}, \quad (6)$$

where $\mathbf{c}_i = (c_{i,1}, c_{i,2}, \dots, c_{i,n}) \in \mathbb{F}_q^n$, for $i = 1, 2, \dots, m$, are the unique vectors in \mathbb{F}_q^n such that $\mathbf{c} = \sum_{i=1}^m \alpha_i \mathbf{c}_i$. The map $M_\alpha : \mathbb{F}_q^{m \times n} \rightarrow \mathbb{F}_q^{m \times n}$ is an \mathbb{F}_q -linear vector space isomorphism.

Recall that a q -linearized polynomial over \mathbb{F}_q^m is a polynomial of the form $F(x) = \sum_{i=0}^d F_i x^{q^i}$, where $F_i \in \mathbb{F}_q^m$. Denote also $\text{ev}_\alpha(F(x)) = (F(\alpha_1), F(\alpha_2), \dots, F(\alpha_n)) \in \mathbb{F}_q^n$,

and finally define

$$\mathcal{C}_2 = \{M_\alpha(\text{ev}_\alpha(F(x))) \mid F_i = 0 \text{ for } i < k_1 - k_2 \text{ and } i \geq k_1\},$$

$$\mathcal{C}_1 = \{M_\alpha(\text{ev}_\alpha(F(x))) \mid F_i \in \mathcal{H}_i \text{ for } 0 \leq i < k_1 - k_2,$$

$$F_i \in \mathbb{F}_q^m \text{ for } k_1 - k_2 \leq i < k_1, F_i = 0 \text{ for } i \geq k_1\},$$

where $\mathcal{H}_0, \mathcal{H}_1, \dots, \mathcal{H}_{k_1-k_2-1} \subseteq \mathbb{F}_q^m$ are the \mathbb{F}_q -linear vector spaces described in [11, Theorem 8].

A secret message is a vector $\mathbf{x} \in \mathcal{H}_0 \times \mathcal{H}_1 \times \dots \times \mathcal{H}_{k_1-k_2-1}$, and the encoding is as follows: choose uniformly at random a q -linearized polynomial $F(x) = \sum_{i=0}^{k_1-1} F_i x^{q^i}$ over \mathbb{F}_q^m such that $\mathbf{x} = (F_0, F_1, \dots, F_{k_1-k_2-1})$.

Now we prove the previous three items:

- 1) The information parameter ℓ coincides with the dimension of the linear code

$$\mathcal{W} = \{M_\alpha(\text{ev}_\alpha(F(x))) \mid F_i \in \mathcal{H}_i \text{ for } i < k_1 - k_2$$

$$\text{and } F_i = 0 \text{ for } i \geq k_1 - k_2\},$$

which is at least $m(k_1 - k_2)(1 - 2\varepsilon)$ by [11, Theorem 8], as explained in [11, page 2713].

- 2) By Theorem 3, the security parameter is $t = d_R(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp) - 1 \geq d_R(\mathcal{C}_2^\perp) - 1$. Since \mathcal{C}_2 is MRD, then so is its trace dual [5], which means that $d_R(\mathcal{C}_2^\perp) = k_2 + 1$, and the result follows.
- 3) We first perform list-decoding using the code \mathcal{C}_1 , and obtain in polynomial time a list that is an $(s - 1, m/n, k_1)$ -periodic subspace of $\mathbb{F}_q^{k_1}$ by [11, Lemma 16] (recall the definition of periodic subspace from [11, Definition 9]).

Project this periodic subspace onto the first $k_1 - k_2$ coordinates, which still gives a periodic subspace, and intersect it with $\mathcal{H}_0 \times \mathcal{H}_1 \times \dots \times \mathcal{H}_{k_1-k_2-1}$. Such intersection is an \mathbb{F}_q -linear affine space of dimension at most $O(s^2/\varepsilon^2)$, as in the proof of [11, Theorem 17], and hence the result follows.

VI. BASIC PROPERTIES OF RGMWS

We give now upper and lower Singleton-type bounds on RGMWs of nested linear code pairs:

Theorem 5 (Upper Singleton bound). *Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$ and $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$, it holds that*

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \leq n - \left\lceil \frac{\ell - r + 1}{m} \right\rceil + 1. \quad (7)$$

In particular, it follows that

$$\dim(\mathcal{C}_1/\mathcal{C}_2) \leq \max\{m, n\}(\min\{m, n\} - d_R(\mathcal{C}_1, \mathcal{C}_2) + 1).$$

Proof: First, we have that $d_{M,\ell}(\mathcal{C}_1, \mathcal{C}_2) \leq n$ by definition. For the general case, it is enough to prove that $md_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \leq mn - \ell + r + m - 1$. Assume that $1 \leq r \leq \ell - hm$, where the integer $h \geq 0$ is the maximum possible. That is, $r + (h + 1)m > \ell$. Using Proposition 3, we obtain

$$md_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \leq md_{M,r+hm}(\mathcal{C}_1, \mathcal{C}_2) - hm$$

$$\leq md_{M,\ell}(\mathcal{C}_1, \mathcal{C}_2) - hm \leq mn - \ell + r + m - 1,$$

where the last inequality follows from $md_{M,\ell}(\mathcal{C}_1, \mathcal{C}_2) \leq mn$ and $r + (h + 1)m - 1 \geq \ell$. \blacksquare

Theorem 6 (Lower Singleton bound). *Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$ and $1 \leq r \leq \dim(\mathcal{C}_1/\mathcal{C}_2)$, it holds that $md_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \geq r$, which implies that*

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \geq \left\lceil \frac{r}{m} \right\rceil. \quad (8)$$

Proof: Take a subspace $\mathcal{D} \subseteq \mathbb{F}^{m \times n}$ and define $\mathcal{L} = \text{RSupp}(\mathcal{D})$. Using (1), we see that

$$m \text{wt}_R(\mathcal{D}) = m \dim(\mathcal{L}) = \dim(\mathcal{V}_{\mathcal{L}}) \geq \dim(\mathcal{D}).$$

The result follows from this and Theorem 2. \blacksquare

On the other hand, it is well-known that, in the Hamming case, all generalized Hamming weights of a linear code determine uniquely those of the corresponding dual code. This is known as Wei's Duality Theorem [27, Theorem 3]. Next we give an analogous result for the generalized matrix weights of a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ and its dual \mathcal{C}^\perp . See [19] for a proof.

Theorem 7 (Duality theorem). *Given a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ with $k = \dim(\mathcal{C})$, and given an integer $p \in \mathbb{Z}$, define*

$$W_p(\mathcal{C}) = \{d_{M,p+rm}(\mathcal{C}) \mid r \in \mathbb{Z}, 1 \leq p+rm \leq k\},$$

$$\overline{W}_p(\mathcal{C}) = \{n+1-d_{M,p+rm}(\mathcal{C}) \mid r \in \mathbb{Z}, 1 \leq p+rm \leq k\}.$$

Then it holds that

$$\{1, 2, \dots, n\} = W_p(\mathcal{C}^\perp) \cup \overline{W}_{p+k}(\mathcal{C}),$$

where the union is disjoint.

VII. SECURITY EQUIVALENCES OF LINEAR COSET CODING SCHEMES AND MINIMUM PARAMETERS

In this section, we study when two nested linear code pairs $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$ and $\mathcal{C}'_2 \subsetneq \mathcal{C}'_1 \subseteq \mathbb{F}^{m' \times n'}$ have the same security and reliability performance, meaning they perform equally regarding information leakage and error correction.

In this sense, we conclude the section by studying the minimum possible parameters m and n for a linear code, which correspond to the packet length and the number of outgoing links from the source node (see Subsection II-B).

A vector space isomorphism preserves full-secrecy thresholds if it is a rank isometry, due to Theorem 3. On the other hand, it completely preserves the security behaviour of linear coset coding schemes if it preserves rank support spaces, in view of Proposition 4. This motivates the following definitions:

Definition 10 (Rank isometries and security equivalences).

We say that a vector space isomorphism $\phi : \mathcal{V} \rightarrow \mathcal{W}$ between rank support spaces $\mathcal{V} \in RS(\mathbb{F}^{m \times n})$ and $\mathcal{W} \in RS(\mathbb{F}^{m' \times n'})$ is a rank isometry if $\text{Rk}(\phi(V)) = \text{Rk}(V)$, for all $V \in \mathcal{V}$, and we say that it is a security equivalence if $\mathcal{U} \subseteq \mathcal{V}$ is a rank support space if, and only if, $\phi(\mathcal{U}) \subseteq \mathcal{W}$ is a rank support space.

Two nested linear code pairs $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$ and $\mathcal{C}'_2 \subsetneq \mathcal{C}'_1 \subseteq \mathbb{F}^{m' \times n'}$ are said to be security equivalent if there exist rank support spaces $\mathcal{V} \in RS(\mathbb{F}^{m \times n})$ and $\mathcal{W} \in RS(\mathbb{F}^{m' \times n'})$, containing \mathcal{C}_1 and \mathcal{C}'_1 , respectively, and a security equivalence $\phi : \mathcal{V} \rightarrow \mathcal{W}$ with $\phi(\mathcal{C}_1) = \mathcal{C}'_1$ and $\phi(\mathcal{C}_2) = \mathcal{C}'_2$.

The following result is inspired by [18, Theorem 5], which treats a particular case. See [19] for a proof.

Theorem 8. *Let $\phi : \mathcal{V} \rightarrow \mathcal{W}$ be a vector space isomorphism between rank support spaces $\mathcal{V} \in RS(\mathbb{F}^{m \times n})$ and $\mathcal{W} \in RS(\mathbb{F}^{m' \times n'})$, and consider the following properties:*

- (P 1) *There exist full-rank matrices $A \in \mathbb{F}^{m \times m}$ and $B \in \mathbb{F}^{n \times n'}$ such that $\phi(C) = ACB$, for all $C \in \mathcal{V}$.*
- (P 2) *ϕ is a security equivalence.*
- (P 3) *For all subspaces $\mathcal{D} \subseteq \mathcal{V}$, it holds that $\text{wt}_R(\phi(\mathcal{D})) = \text{wt}_R(\mathcal{D})$.*
- (P 4) *ϕ is a rank isometry.*

Then the following implications hold:

$$(P 1) \iff (P 2) \iff (P 3) \implies (P 4).$$

In particular, a security equivalence is a rank isometry and, in the case $\mathcal{V} = \mathcal{W} = \mathbb{F}^{m \times n}$ and $m \neq n$, the converse holds.

Remark 2. *Unfortunately, the implication $(P 3) \iff (P 4)$ not always holds. Take for instance $m = n$ and the map $\phi : \mathbb{F}^{m \times m} \rightarrow \mathbb{F}^{m \times m}$ given by $\phi(C) = C^T$, for all $C \in \mathbb{F}^{m \times m}$.*

The following consequence shows the minimum parameters of a linear code and can be seen as an extension of [18, Proposition 3].

Proposition 6. *For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ of dimension k , the following hold:*

- 1) *There exists a linear code $\mathcal{C}' \subseteq \mathbb{F}^{m' \times n'}$ that is security equivalent to \mathcal{C} if, and only if, $n' \geq d_{M,k}(\mathcal{C})$.*
- 2) *If $m' \geq d_{M,k}(\mathcal{C}^T)$, then there exists a linear code $\mathcal{C}' \subseteq \mathbb{F}^{m' \times n}$ that is rank isometric to \mathcal{C} , where*

$$\mathcal{C}^T = \{C^T \mid C \in \mathcal{C}\} \subseteq \mathbb{F}^{n \times m}.$$

VIII. RELATION WITH OTHER EXISTING NOTIONS OF GENERALIZED WEIGHTS

In this section, we study the relation between RGMWs and other notions of generalized weights. In particular, we consider the classical generalized Hamming weights [27], relative generalized Hamming weights [17], relative generalized rank weights [15], [20] and Delsarte generalized weights [23].

We also compare RDRPs with the relative dimension/length profile from [8], [17] and the relative dimension/intersection profile from [15].

A. RGMWs extend relative generalized rank weights

In this subsection, we prove that RGMWs extend the relative generalized rank weights defined in [15].

Throughout the subsection, we will consider the extension field \mathbb{F}_{q^m} of the finite field \mathbb{F}_q , and vector spaces in $\mathbb{F}_{q^m}^n$ will be considered to be linear over \mathbb{F}_{q^m} . We need first the notion of Galois closed spaces [26]:

Definition 11 (Galois closed spaces [26]). We say that an \mathbb{F}_{q^m} -linear vector space $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ is Galois closed if

$$\mathcal{V}^q = \{(v_1^q, v_2^q, \dots, v_n^q) \mid (v_1, v_2, \dots, v_n) \in \mathcal{V}\} \subseteq \mathcal{V}.$$

We denote by $\Upsilon(\mathbb{F}_{q^m}^n)$ the family of \mathbb{F}_{q^m} -linear Galois closed vector spaces in $\mathbb{F}_{q^m}^n$.

Definition 12 (Relative Dimension/Intersection Profile [15, Definition 1]). Given nested \mathbb{F}_{q^m} -linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq$

$\mathbb{F}_{q^m}^n$, and $0 \leq \mu \leq n$, we define their μ -th relative dimension/intersection profile (RDIP) as

$$K_{R,\mu}(\mathcal{C}_1, \mathcal{C}_2) = \max\{\dim(\mathcal{C}_1 \cap \mathcal{V}) - \dim(\mathcal{C}_2 \cap \mathcal{V}) \mid \mathcal{V} \in \Upsilon(\mathbb{F}_{q^m}^n), \dim(\mathcal{V}) \leq \mu\},$$

where dimensions are taken over \mathbb{F}_{q^m} .

Definition 13 (Relative Generalized Rank Weights [15, Definition 2]). Given nested \mathbb{F}_{q^m} -linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, and $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$ (over \mathbb{F}_{q^m}), we define their r -th relative generalized rank weight (RGRW) as

$$d_{R,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{\dim(\mathcal{V}) \mid \mathcal{V} \in \Upsilon(\mathbb{F}_{q^m}^n), \dim(\mathcal{C}_1 \cap \mathcal{V}) - \dim(\mathcal{C}_2 \cap \mathcal{V}) \geq r\},$$

where dimensions are taken over \mathbb{F}_{q^m} .

We may now show the following characterization. Recall the matrix representation map from (6).

Theorem 9. Let $\alpha_1, \alpha_2, \dots, \alpha_m$ be a basis of \mathbb{F}_{q^m} as a vector space over \mathbb{F}_q , and let $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ be an arbitrary set. The following are equivalent:

- 1) $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ is an \mathbb{F}_{q^m} -linear Galois closed vector space.
- 2) $M_\alpha(\mathcal{V}) \subseteq \mathbb{F}_q^{m \times n}$ is a rank support space.

Moreover, if $M_\alpha(\mathcal{V}) = \mathcal{V}_\mathcal{L}$ for a subspace $\mathcal{L} \subseteq \mathbb{F}^n$, then

$$\dim(\mathcal{V}) = \dim(\mathcal{L}),$$

where $\dim(\mathcal{V})$ is taken over \mathbb{F}_{q^m} .

Proof: For an arbitrary set $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$, [26, Lemma 1] states that \mathcal{V} is an \mathbb{F}_{q^m} -linear Galois closed vector space if, and only if, \mathcal{V} is \mathbb{F}_q -linear and it has a basis over \mathbb{F}_q of the form $\mathbf{v}_{i,j} = \alpha_i \mathbf{b}_j$, for $i = 1, 2, \dots, m$ and $j = 1, 2, \dots, k$, where $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_k \in \mathbb{F}_q^n$. By considering $B_{i,j} = M_\alpha(\mathbf{v}_{i,j}) \in \mathbb{F}_q^{m \times n}$, we see that this condition is equivalent to item 2 in Theorem 1, and we are done. ■

Therefore, the following result follows:

Corollary 1. Let $\alpha_1, \alpha_2, \dots, \alpha_m$ be a basis of \mathbb{F}_{q^m} as a vector space over \mathbb{F}_q . Given nested \mathbb{F}_{q^m} -linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, and integers $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$ (over \mathbb{F}_{q^m}), $0 \leq p \leq m-1$ and $0 \leq \mu \leq n$, we have that

$$d_{R,r}(\mathcal{C}_1, \mathcal{C}_2) = d_{M,r-m-p}(M_\alpha(\mathcal{C}_1), M_\alpha(\mathcal{C}_2)),$$

$$mK_{R,\mu}(\mathcal{C}_1, \mathcal{C}_2) = K_{M,\mu}(M_\alpha(\mathcal{C}_1), M_\alpha(\mathcal{C}_2)).$$

B. RGMWs extend relative generalized Hamming weights

In this subsection, we show that relative generalized matrix weights also extend relative generalized Hamming weights [17], and therefore generalized matrix weights extend generalized Hamming weights [27]. We start with the definitions of Hamming supports and Hamming support spaces:

Definition 14 (Hamming supports). Given a vector space $\mathcal{C} \subseteq \mathbb{F}^n$, we define its Hamming support as

$$\text{HSupp}(\mathcal{C}) = \{i \in \{1, 2, \dots, n\} \mid \exists (c_1, c_2, \dots, c_n) \in \mathcal{C}, c_i \neq 0\}.$$

We also define the Hamming weight of the space \mathcal{C} as

$$\text{wt}_H(\mathcal{C}) = \#\text{HSupp}(\mathcal{C}).$$

Definition 15 (Hamming support spaces). Given a subset $I \subseteq \{1, 2, \dots, n\}$, we define its Hamming support space as

the vector space in \mathbb{F}^n given by

$$\mathcal{L}_I = \{(c_1, c_2, \dots, c_n) \in \mathbb{F}^n \mid c_i = 0, \forall i \notin I\}.$$

We may now define relative generalized Hamming weights and relative dimension/length profile:

Definition 16 (Relative Dimension/Length Profile [8], [17]). Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^n$, and $0 \leq \mu \leq n$, we define their μ -th relative dimension/length profile (RDLP) as

$$K_{H,\mu}(\mathcal{C}_1, \mathcal{C}_2) = \max\{\dim(\mathcal{C}_1 \cap \mathcal{L}_I) - \dim(\mathcal{C}_2 \cap \mathcal{L}_I) \mid I \subseteq \{1, 2, \dots, n\}, \#I \leq \mu\}.$$

Definition 17 (Relative Generalized Hamming Weights [17, Section III]). Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^n$, and $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$, we define their r -th relative generalized Hamming weight (RGHW) as

$$d_{H,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{\#I \mid I \subseteq \{1, 2, \dots, n\}, \dim(\mathcal{C}_1 \cap \mathcal{L}_I) - \dim(\mathcal{C}_2 \cap \mathcal{L}_I) \geq r\}.$$

We will now show how to see vectors in \mathbb{F}^n as matrices in $\mathbb{F}^{n \times n}$. To that end, we introduce the diagonal matrix representation map $\Delta : \mathbb{F}^n \rightarrow \mathbb{F}^{n \times n}$ given by

$$\Delta(\mathbf{c}) = \text{diag}(\mathbf{c}) = (c_i \delta_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}, \quad (9)$$

where $\mathbf{c} = (c_1, c_2, \dots, c_n) \in \mathbb{F}^n$ and $\delta_{i,j}$ represents the Kronecker delta. In other words, $\Delta(\mathbf{c})$ is the diagonal matrix whose diagonal vector is \mathbf{c} .

Clearly Δ is linear and one to one. Moreover, we have the following properties.

Proposition 7. Let $\mathcal{D} \subseteq \mathbb{F}^n$ be a vector space, and let $I \subseteq \{1, 2, \dots, n\}$ be a set. Defining $J = \text{HSupp}(\mathcal{D}) \subseteq \{1, 2, \dots, n\}$, the following properties hold:

- 1) $\text{RSupp}(\Delta(\mathcal{D})) = \mathcal{L}_J \subseteq \mathbb{F}^n$.
- 2) For a rank support space $\mathcal{V} \subseteq \mathbb{F}^{n \times n}$, if $\Delta(\mathcal{D}) = \mathcal{V} \cap \Delta(\mathbb{F}^n)$, then $\mathcal{D} = \mathcal{L}_J$.
- 3) $\text{wt}_R(\Delta(\mathcal{D})) = \text{wt}_H(\mathcal{D})$.

Therefore, the following result holds:

Corollary 2. Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^n$, and integers $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$ and $0 \leq \mu \leq n$, we have that

$$d_{H,r}(\mathcal{C}_1, \mathcal{C}_2) = d_{M,r}(\Delta(\mathcal{C}_1), \Delta(\mathcal{C}_2)),$$

$$K_{H,\mu}(\mathcal{C}_1, \mathcal{C}_2) = K_{M,\mu}(\Delta(\mathcal{C}_1), \Delta(\mathcal{C}_2)).$$

C. GMWs improve Delsarte generalized weights

A notion of generalized weights, called Delsarte generalized weights, for a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ has already been proposed in [23]. We will prove that generalized matrix weights are larger than or equal to Delsarte generalized weights for an arbitrary linear code, and we will prove that the inequality is strict for some linear codes.

These weights are defined in terms of optimal anticodes for the rank metric:

Definition 18 (Maximum rank distance). For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$, we define its maximum rank distance as

$$\text{MaxRk}(\mathcal{C}) = \max\{\text{Rk}(\mathcal{C}) \mid \mathcal{C} \in \mathcal{C}, \mathcal{C} \neq \emptyset\}.$$

The following bound is given in [22, Proposition 47]:

$$\dim(\mathcal{C}) \leq m \text{MaxRk}(\mathcal{C}). \quad (10)$$

This leads to the definition of rank-metric optimal anticodes:

Definition 19 (Optimal anticodes [23, Definition 22]). We say that a linear code $\mathcal{V} \subseteq \mathbb{F}^{m \times n}$ is a (rank-metric) optimal anticode if equality in (10) holds.

We will denote by $A(\mathbb{F}^{m \times n})$ the family of linear optimal anticodes in $\mathbb{F}^{m \times n}$.

In view of this, Delsarte generalized weights are defined in [23] as follows:

Definition 20 (Delsarte generalized weights [23, Definition 23]). For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ and an integer $1 \leq r \leq \dim(\mathcal{C})$, we define its r -th Delsarte generalized weight (DGW) as

$$d_{D,r}(\mathcal{C}) = m^{-1} \min\{\dim(\mathcal{V}) \mid \mathcal{V} \in A(\mathbb{F}^{m \times n}), \dim(\mathcal{C} \cap \mathcal{V}) \geq r\}.$$

We have that rank support spaces are optimal anticodes, which can be seen as [23, Theorem 18] due to Theorem 9.

Proposition 8 ([23, Theorem 18]). *If a set $\mathcal{V} \subseteq \mathbb{F}^{m \times n}$ is a rank support space, then it is a (rank-metric) optimal anticode. In other words, $RS(\mathbb{F}^{m \times n}) \subseteq A(\mathbb{F}^{m \times n})$.*

Thus, the next consequence follows from the previous proposition and the corresponding definitions:

Corollary 3. *For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ and an integer $1 \leq r \leq \dim(\mathcal{C})$, we have that*

$$d_{D,r}(\mathcal{C}) \leq d_{M,r}(\mathcal{C}).$$

However, $RS(\mathbb{F}^{m \times n}) \subsetneq A(\mathbb{F}^{m \times n})$ in general and, in some cases, generalized matrix weights are strictly larger than Delsarte generalized weights. Consider, for instance, $m = n = 2$ and the linear code

$$\mathcal{C} = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\rangle \subseteq \mathbb{F}^{2 \times 2}.$$

It holds that \mathcal{C} is a linear optimal anticode, but it is not a rank support space. Moreover, $d_{D,2}(\mathcal{C}) = 1$ and $d_{M,2}(\mathcal{C}) = 2$.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the support from The Danish Council for Independent Research (Grant No. DFF-4002-00367) and from the Japan Society for the Promotion of Science (Grant No. 26289116). The first author is also thankful for the support and guidance of his advisors Olav Geil and Diego Ruano.

REFERENCES

- [1] R. Ahlswede, N. Cai, S. Y. R. Li, and R. W. Yeung. Network information flow. *IEEE Trans. Inf. Theory*, 46(4):1204–1216, July 2000.
- [2] N. Cai and R. W. Yeung. Network coding and error correction. *Proc. 2002 IEEE Inform. Theory Workshop*, pages 119–122, 2002.
- [3] N. Cai and R. W. Yeung. Secure network coding. In *Proceedings of the IEEE International Symposium on Information Theory*, pages 323–, 2002.
- [4] T. M. Cover and J. A. Thomas. *Elements of Information Theory* (Wiley Series in Telecommunications and Signal Processing). Wiley-Interscience, 2006.
- [5] Ph. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A*, 25(3):226 – 241, 1978.
- [6] S. El Rouayheb, E. Soljanin, and A. Sprintson. Secure network coding for wiretap networks of type II. *IEEE Trans. Inf. Theory*, 58(3):1361–1371, March 2012.
- [7] J. Feldman, T. Malkin, R. Servedio, and C. Stein. On the capacity of secure network coding. In *Proceedings of the 42nd Annual Allerton Conference on Communication, Control, and Computing*, 2004.
- [8] G. D. Forney Jr. Dimension/length profiles and trellis complexity of linear block codes. *IEEE Trans. Inf. Theory*, 40(6):1741–1752, 1994.
- [9] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problems Inform. Transmission*, 21, 1985.
- [10] E. M. Gabidulin, A. V. Ourivski, B. Honary, and B. Ammar. Reducible rank codes and their applications to cryptography. *IEEE Trans. Inf. Theory*, 49(12):3289–3293, Dec 2003.
- [11] V. Guruswami, C. Wang, and C. Xing. Explicit list-decodable rank-metric and subspace codes via subspace designs. *IEEE Trans. Inf. Theory*, 62(5):2707–2718, May 2016.
- [12] T. Ho, M. Medard, R. Koetter, D.R. Karger, M. Effros, J. Shi, and B. Leong. A random linear network coding approach to multicast. *IEEE Trans. Inf. Theory*, 52(10):4413–4430, Oct 2006.
- [13] R. Jurius and R. Pellikaan. On defining generalized rank weights. *arXiv:1506.02865*, 2015.
- [14] R. Kötter and M. Medard. An algebraic approach to network coding. *IEEE/ACM Trans. Networking*, 11(5):782–795, Oct 2003.
- [15] J. Kurihara, R. Matsumoto, and T. Uyematsu. Relative generalized rank weight of linear codes and its applications to network coding. *IEEE Trans. Inf. Theory*, 61(7):3912–3936, July 2015.
- [16] S. Y. R. Li, R.W. Yeung, and N. Cai. Linear network coding. *IEEE Trans. Inf. Theory*, 49(2):371–381, Feb 2003.
- [17] Y. Luo, C. Mitropant, A. J. Han Vinck, and K. Chen. Some new characters on the wire-tap channel of type II. *IEEE Trans. Inf. Theory*, 51(3):1222–1229, 2005.
- [18] U. Martínez-Peñas. On the similarities between generalized rank and Hamming weights and their applications to network coding. *IEEE Trans. Inf. Theory*, 62(7):4081–4095, 2016.
- [19] U. Martínez-Peñas and R. Matsumoto. Unifying notions of generalized weights for universal security on wire-tap networks. *arXiv:1607.01263*, 2016.
- [20] F. E. Oggier and A. Sboui. On the existence of generalized rank weights. In *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012*, pages 406–410, 2012.
- [21] L. H. Ozarow and A. D. Wyner. Wire-tap channel II. chapter Advances in Cryptology: Proceedings of EUROCRYPT 84 A Workshop on the Theory and Application of Cryptographic Techniques Paris, France, April 9– 11, 1984, pages 33–50. Springer Berlin Heidelberg, Berlin, Heidelberg, 1985.
- [22] A. Ravagnani. Rank-metric codes and their duality theory. *Designs, Codes and Cryptography*, pages 1–20, 2015.
- [23] A. Ravagnani. Generalized weights: An anticode approach. *Journal of Pure and Applied Algebra*, 220(5):1946 – 1962, 2016.
- [24] D. Silva and F. R. Kschischang. On metrics for error correction in network coding. *IEEE Trans. Inf. Theory*, 55(12):5479–5490, 2009.
- [25] D. Silva and F. R. Kschischang. Universal secure network coding via rank-metric codes. *IEEE Trans. Inf. Theory*, pages 1124–1135, 2011.
- [26] H. Stichtenoth. On the dimension of subfield subcodes. *IEEE Trans. Inf. Theory*, 36(1):90–93, Jan 1990.
- [27] V. K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inf. Theory*, 37(5):1412–1418, 1991.
- [28] A. D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, Oct 1975.
- [29] R. Zamir, S. Shamai, and U. Erez. Nested linear/lattice codes for structured multiterminal binning. *IEEE Trans. Inf. Theory*, 48(6):1250–1276, Jun 2002.